5G biztonság – közös felelősség

A digitális bizalom fontosabb, mint valaha

Cserháti Vencel

2022. szeptember 29., Budapest

A feltörekvő technológiák a digitális növekedés motorjai, de az új lehetőségek új kihívásokat is jelentenek

Új technológiai trendek

Felhő

SDN/NFV

AI

5G

IoT

Új lehetőségek

A felhőtechnológiák használata lehetővé teszi az erőforrások megosztását és a szolgáltatási platformok zártból nyílt platformmá alakulását.

A mesterséges intelligencia és a nagy mennyiségű adatok mélyreható információbányászatot tesznek lehetővé.

A mobilhálózatok és a szenzorok használata nagy sűrűségű összeköttetéshálózatra ad lehetőséget.

Új kihívások

1. A hagyományos védelmi határvonal egyre inkább elmosódik.
2. Az adatfeldolgozás egyre összetettebb, és az adatszivárgás kockázata növekszik.
3. A támadási felület egyre nagyobb, és a sebezhetőségek egyre nőnek.
4. Vannak politikai tényezők, amik befolyásolják a döntéseket

A kiberbiztonság nemcsak technológiai és irányítási kérdésekről szól, hanem jogról, értékekről és pszichoszociális kérdésekről is.

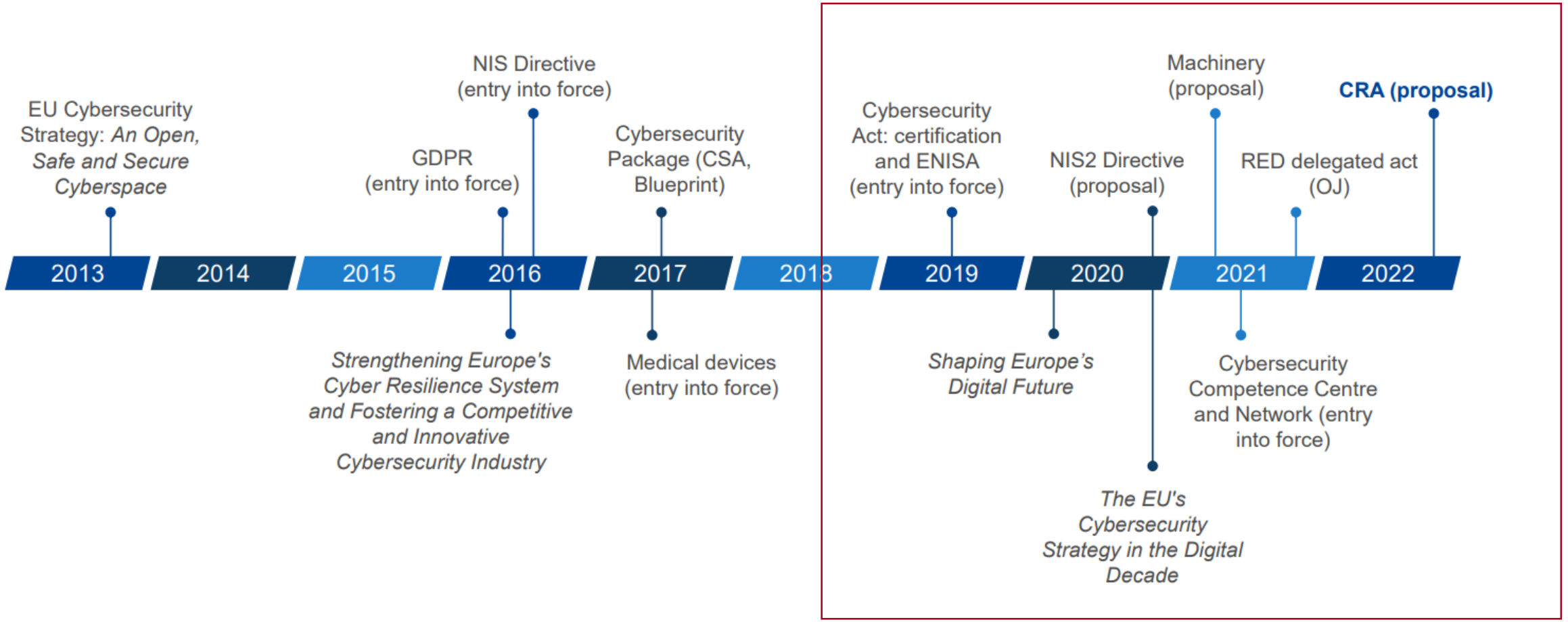
Ha a polgári légi közlekedés biztonsági rendszerében nem bízunk, ki mer majd repülni?

Egy ilyen rendszer felépítéséhez a repülőgépgyártók, a légitársaságok, a repülőterek, az utasok mind hozzájárulnak...

A biztonsági előírások, szabványok, intézkedések, a biztonsági kultúra magától értetődőnek számítanak...

HUAWEI

Hogyan reagáljunk a kihívásokra? Az EU több kiberbiztonsági jogszabályról is tárgyal



HUAWEI

Az Európai Bizottság számos jogalkotási javaslatot tett a kibertámadásokra válaszul

Kiberbiztonsági törvény (2019)

- Hatályba lépett 2019. június 27-én
- Két célkitűzése van:
- **az ENISA megerősítése** az EU tagállamainak támogatása a kiberbiztonsági fenyegetésekkel szembeni fellépésben; és
- **Az egész EU-ra kiterjedő kiberbiztonsági tanúsítási keretrendszer (ECCF) létrehozása, amelyben az** ENISA és az Európai Bizottság kulcsszerepet fog játszani.

Napokkal azután, hogy az Európai Gyógyszerügynökség elleni kibertámadás két Covid-19 vakcinával kapcsolatos érzékeny információkat hozott nyilvánosságra, és egy olyan pillanatban, amikor a SolarWinds betörése a valaha volt talán legkövetkezetesebb kiberincidenssé válik, amely minden ágazatban, a közigazgatásban és a kormányoknál világszerte érinti a vállalkozásokat.....

Kiberbiztonsági stratégia

Frissített kiberbiztonsági stratégia, amely részletes munkatervet tartalmaz az Európai Bizottság, a tagállamok és az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) számára az 5G és a hálózatbiztonság terén történő előrelépéshez, többek között:

- **Új mechanizmusok az** iparági szereplők, valamint a köz- és biztonsági hatóságok számára **a fenyegetésekkel kapcsolatos információk és az incidensekre adott válaszlépésekkel kapcsolatos információk cseréje érdekében.**
- **Számos intézkedés az uniós intézmények és ügynökségek számára az adataik jobb védelme érdekében,** miután évek óta egyre több aggodalom merül fel az EU diplomáciai kommunikációjával biztonságával kapcsolatban.

NIS2-irányelv

- A NIS2 javaslat a hálózati és információs rendszerek biztonságáról szóló irányelv felülvizsgálatát követően készült el.
- **Többek között a nemzeti szintű kiberbiztonsági képességek fejlesztése; fokozott uniós szintű együttműködés.**
- **Sokkal szélesebb hatály** - az "alapvető" és "fontos" szervezetekre vonatkozó követelmények (az I. és II. mellékletben meghatározottak szerint).
- Több hatáskör az EU hálózat- és információbiztonsággal foglalkozó együttműködési csoportjának, az ENISA-nak, a CSIRT-eknek és a tagállami hatóságoknak.

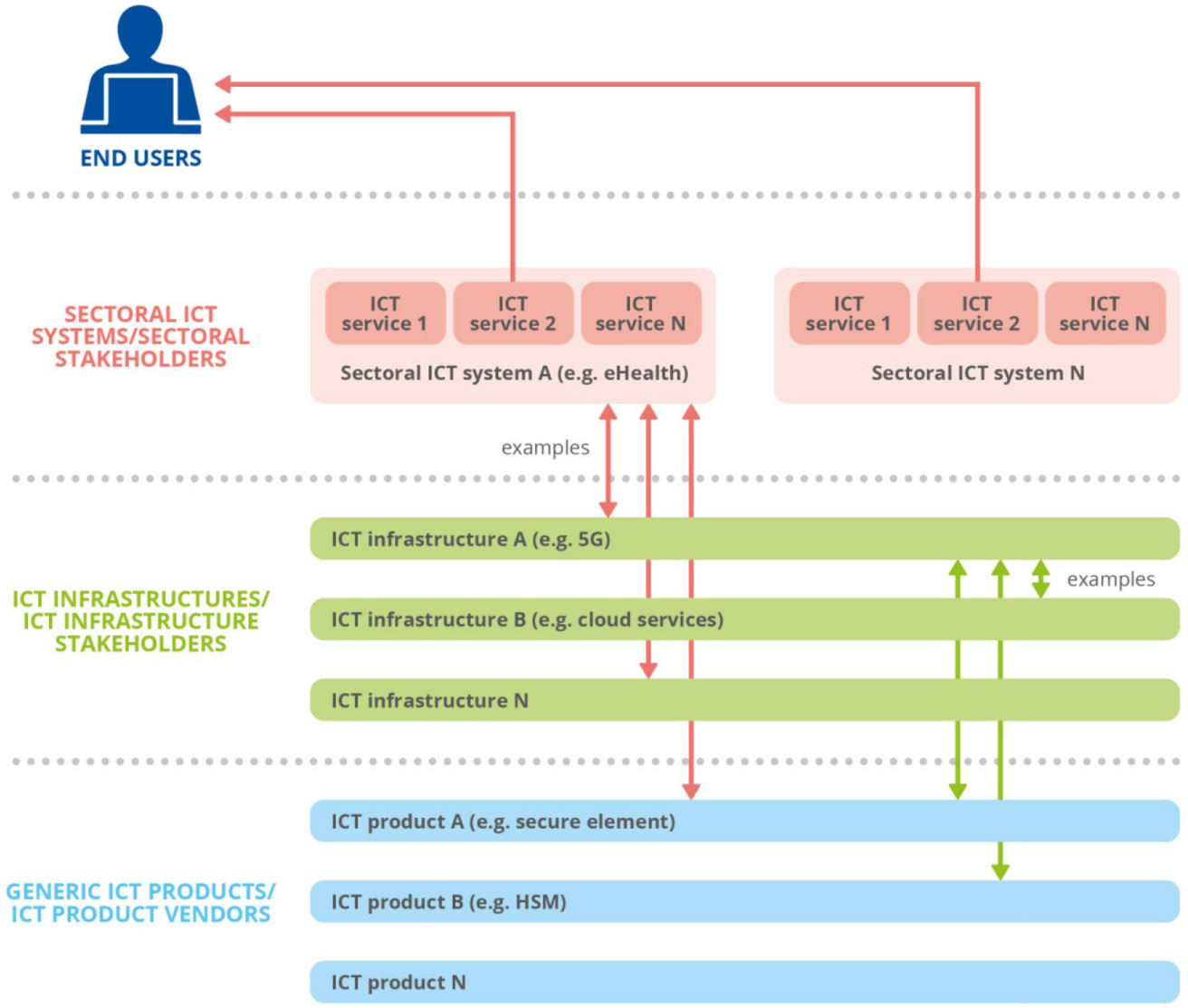
CRA javaslat

Kiberbiztonságról szóló törvény (CRA)

- A "digitális elemeket tartalmazó termékekre" vonatkozó szabályok a megfelelő szintű kiberbiztonság biztosítása érdekében; a megfelelőségértékelési eljárások a "kockázat" alapján eltérőek.
- A digitális elemeket tartalmazó termékek tervezésének, fejlesztésének és gyártásának alapvető követelményei.
- A sebezhetőségkezelési folyamatokra és az incidensek jelentésére vonatkozó alapvető követelmények
- A piacfelügyeleti és végrehajtási szabályok

HUAWEI

Ezekkel a kihívásokkal összetett rendszerek összefüggésében kell szembenéznünk



1. A különböző iparági rendszerek magukban foglalják mindazokat a funkciókat, amelyek az adott piaci szektor végfelhasználóinak nyújtott szolgáltatásokhoz szükségesek. Ehhez a rendszerek IKT szolgáltatásokra és infrastruktúrára támaszkodnak.
2. Az IKT-infrastruktúrák számos termékből állnak. A termékek összetett komponensek összessége.
3. A rendszer biztonsága azon múlik, hogy MINDEN szereplő felelősséget vállal-e kötelezettségeiért.
4. A szabványügyi testületek határozzák meg a jó gyakorlatokat. A kormányok és a szabályozó hatóságok ajánlják vagy előírják, illetve felügyelik és ellenőrzik a megfelelést.

Forrás: Az ENISA javasolt módszertana az IPARÁGI KIBERBIZTONSÁGI FELMÉRÉSEKHEZ 2021. szeptember

HUAWEI

A iparágak fejlődése érdekében az 5G hálózatnak magasabb biztonsági követelményeknek kell megfelelnie.

Az 5G számos iparágat támogat, és az 5G biztonsága kritikus fontosságú a termelés és a vállalkozások túlélése szempontjából.

Élő közvetítés

Intelligens vezérlés

Intelligens ipar

Intelligens hálózat

Intelligens mezőgazdaság

Intelligens egészségügyi ellátás

Városi biztonság

Intelligens oktatás

Intelligens vezetés

A biztonság a kulcs az 5G-képes ipari alkalmazások megvalósításához

A szolgáltatás fejlődése:

1. Az ipari alkalmazások az 5G hálózatokon kommunikálnak, a vállalati hálózatok és a szolgáltatói hálózatok pedig integrálódnak.
2. Az alkalmazások szerteágazóak és az iparági követelmények eltérőek.
3. Az UPF-eket a hálózat szélére telepítik a vállalati hálózatokhoz való alacsony késleltetésű csatlakozáshoz.

Biztonsági kihívások:

1. Az 5G hálózat a vállalati hálózati infrastruktúra részévé vált, és azt a vállalatok iparági követelményei alapján kell védeni.
2. Mivel a tapasztalatok és a biztonsági követelmények a vállalkozás szolgáltatásai szerint eltérőek, differenciált védelmi képességeket kell biztosítani.
3. Törekedni kell arra, hogy a vállalati adatokat helyben tárolják és dolgozzák fel, valamint hogy a vállalati alkalmazások és adatok jól védettek legyenek.

Az 5G hálózatok legfontosabb biztonsági kihívásai

Üzleti változások

Az 5G hálózat kibővíti az eMBB URLLC és mMTC szolgáltatásait. Meg kell felelni az iparág magasabb biztonsági követelményeinek.

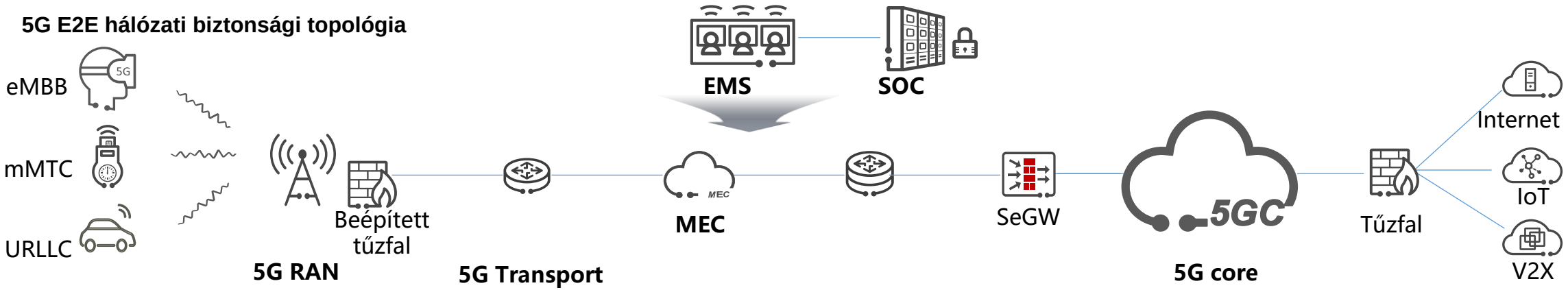
Hálózati változások

Az SBA és a slicing architektúra rugalmas szolgáltatás-kiépítési lehetőségeket biztosít, az UPF downsink pedig támogatja az alacsony késleltetésű szolgáltatásokat, de a hálózati határokat is összetetté és dinamikussá teszi.

Technológiai változás

Az új technológiák, például a virtualizáció és a felhőszolgáltatások alkalmazása támogatja a szolgáltatások gyors bevezetését, de a maghálózat is rétegzetté és szétválasztottá válik.

5G E2E hálózati biztonsági topológia



HUAWEI

Az 5G biztonságossá tétele

Az 5G biztonság együttműködést igényel. *A folyamat minden résztvevőjének felelősséget kell vállalnia a saját területének védelméért.*

Szabványügyi szervezet

3GPP stb: Biztonsági követelmények és szabványok meghatározása az eszközök és protokollok biztonsága érdekében.

Szolgáltatók: A szolgáltatás végponttól végpontig tartó biztonságának megteremtése és felelősségvállalás az alkalmazások adatbiztonságáért.

Kórház
Gyárak
Gépjárművek
Élő közvetítés
....

Operátorok: Biztonságos és ellenálló hálózat kiépítése, valamint a hálózat és a felhasználói adatok biztonságának érdekében alapos kibervédelem és biztonságos üzemeltetési és karbantartási rendszer bevezetése.

5G biztonsági tudásbázis

Eszközgyártók: Biztonságos termékek és funkciók fejlesztése integrált biztonsági folyamat segítségével az eszközök biztonságának növelése és a sebezhetőségek csökkentése érdekében.

RRU/AAU

BBU/CBU

Maghálózat

NESAS

Kormányzat

Szabályozó ügynökségek

Törvények és rendeletek kidolgozása és felügyelet végrehajtása

A szabványügyi szervezetek és a beszállítók felelősek az eszközök biztonságáért, az üzemeltetők a hálózat ellenálló képességéért és az üzemeltetés biztonságáért, az alkalmazásszolgáltatók pedig a szolgáltatások biztonságáért.

HUAWEI

Az 5G kiberbiztonság legfelső szintű tervezési elvei

L3: Alkalmazásbiztonság: Az adatok titkosítása az alkalmazási rétegben

Biztonsági szabványok és jó gyakorlatok (3GPP, ETSI, IETF stb.)

Műszaki bemenet

L2: L1: Termékbiztonság

1. alapelv
Mélyreható védelem

Védelem a külső határon történő behatolás és az oldalirányú támadások ellen

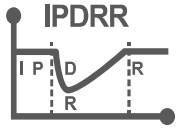
- Anti-DoS (túlterhelés elleni védelem)
- Hozzáférés-ellenőrzés (bejáratvédelem)
- Titkosítás (közzétételi védelem)
- Hamisítás elleni védelem (módosítás elleni védelem)

2. alapelv
Zéró bizalom@5G

Folyamatos értékelés & dinamikus engedélyezés

- Anti-spoofing (hamis kérések azonosítása)
- A kiemelt jogosultság megsértésének megakadályozása (valós kérelmek korlátozása)

3. alapelv
Adaptív biztonság



Dinamikus, folyamatos optimalizálás az IPDRR alapján

- Folyamatos észlelés (anomáliák felfedezése)
- Proaktív zárt hurokszabályozás (anomália-elhárítás)

Biztonsági fejlesztési életciklus (SDL)

Biztonsági értékelés

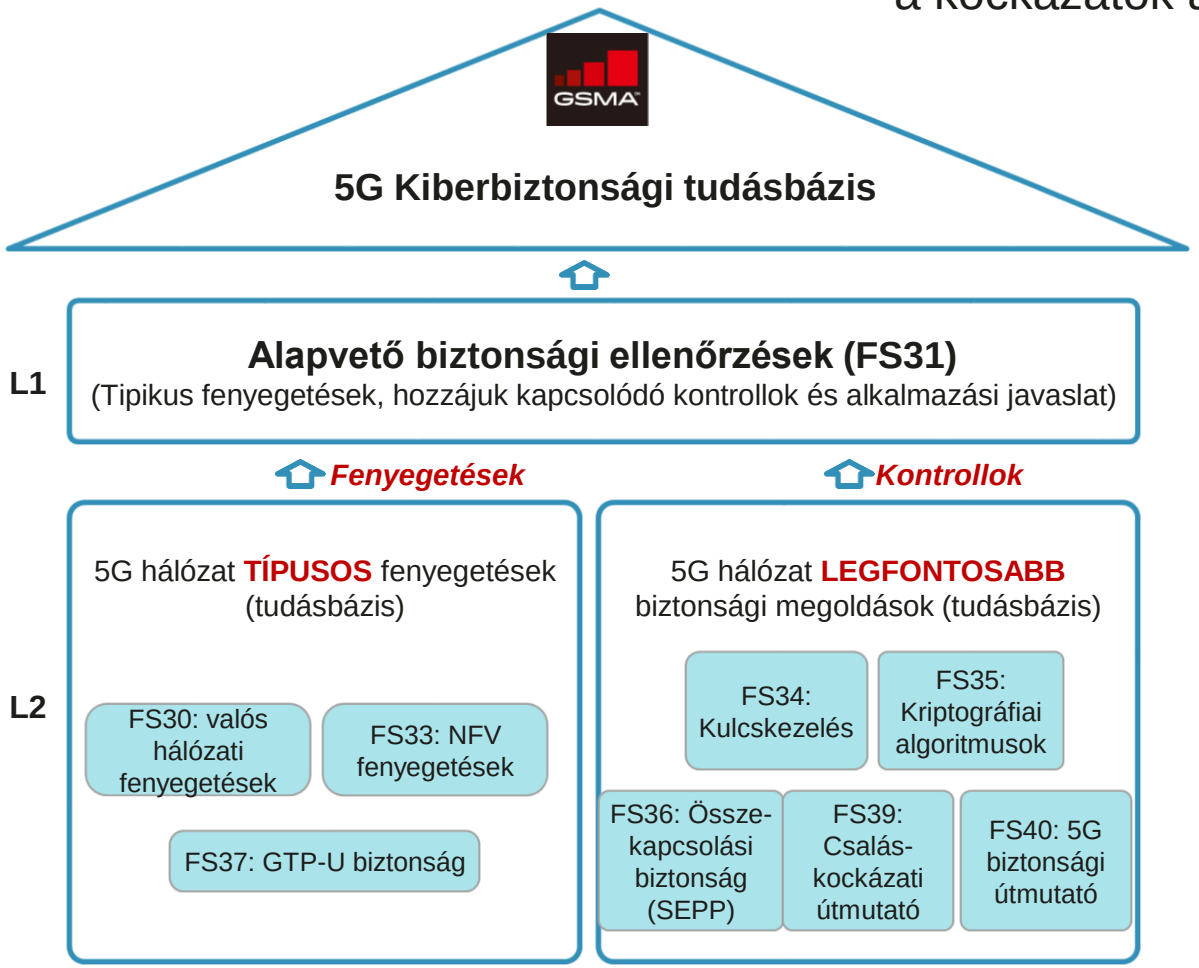
Biztonsági irányítás és felmérés (CC, NESAS, SCAS stb.)

3 rétegű biztonsági modell + 3 biztonsági alapelv, amelyeket a telekommunikációs gyakorlatban eltöltött évek során fejlesztettünk ki.

HUAWEI

Megosztott felelősségvállalás a gyakorlatban: A GSMA kiadta az 5G kiberbiztonsági tudásbázist

A hatékony együttműködés példája az érintett szervezetek számára a kockázatok azonosításához és mérsékléséhez.



MIÉRT:
Cél a kiberbiztonság szintjének javítása, valamint az 5G hálózatokba vetett bizalom erősítése

Mi az?
Dokumentumtár, amely segít az érdekelteknek az 5G kockázatok azonosításában és mérséklésében és tartalmaz

- Átfogó fenyegetéselemzésekből származó inputokat
- Az azonosított fenyegetések kezelésére javasolt biztonsági intézkedéseket, ellenőrzéseket
- A legjobb gyakorlatokra és kockázatcsökkentő intézkedésekre vonatkozó útmutatásokat
- Egyértelmű instrukciókat a kiberbiztonsági megfelelőség eléréséhez

A mobilhálózat-üzemeltetők, a gyártók, a szolgáltatók és a szabályozó hatóságok közreműködésével készült

HUAWEI

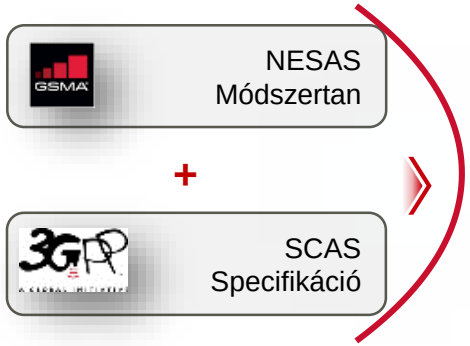
A NESAS-t a szabályozás és a biztonsági követelmények széttagoltságának megoldásának igénye hozta létre

Evolúció

3GPP: Biztonsági értékelési mechanizmus létrehozása	A GSMA által kidolgozott folyamatértékelési kritériumok	NESAS 1.0	NESAS 2.0	NESAS 2.0+
2012	2014	2019.10	2021.02	2021 és azután

Mi a NESAS

- ✓ Egy szabványosított kiberbiztonsági értékelési rendszer
- ✓ A GSMA és a 3GPP által közösen meghatározott
- ✓ A mobilkommunikációs iparág számára kifejlesztve
- ✓ A telekom vállalatok, beszállítók , szabályozók és ipari partnerek bevonása



1. Ellenőrzési folyamat

   A NESAS a termékfejlesztési és életciklusfolyamatok biztonsági auditja.

2. Eszközök tesztelése

   A SCAS teszteseteket biztosít a hálózati eszközök biztonsági értékeléséhez.

Ellenőrzési jelentés

Értékelési jelentés

A NESAS előnyei

- ✓ **Egységesítés:** Az egységes szabványok használatával elkerülhető a széttagoltság és a különböző nemzeti szabályozások és a mobilhálózat-üzemeltetők eltérő biztonsági követelményei által okozott többletköltség.
- ✓ **Technológiai alapú:** Technikai alapkövetelmények meghatározása, amelyek az iparban alkalmazott meghatározó folyamatokon és termékértékelési előírásokon alapulnak.
- ✓ **Folyamatos fejlődés:** Az iparági követelményeken alapuló folyamatos fejlesztés biztosítja a távközlési berendezések biztonságát.

HUAWEI

NESAS ellenőrzési keretrendszer és SCAS előírások

NESAS követelmények

Tervezés	Kódolás	Fordítás	Tesztelés	Release	Operáció	EOX
Req.-01 Tervezett biztonság	Req.-04 Forráskód-felülvizsgálat	Req.-10 Automatizálás	Req.-05 Biztonsági tesztelés	Req.-13 Szoftverintegritás-védelem	Req.-17 Biztonsági kapcsolattartó pont	Req.-12 Sebezhetőségi információk kezelése
N Req.-21 Komponensek beszerzése	Req.-18 Forráskód-menedzsment	Req.-11 Környezet ellenőrzése		Req.-14 Egyedi szoftverkiadási azonosító	Req.-12 Sebezhetőségi információk kezelése	
				Req.-16 Dokumentáció pontossága	Req.-07 A sebezhetőségek javításának folyamata	
				Req.-20 Biztonsági dokumentáció	Req.-08 Sebezhetőség javítás függetlensége	
					Req.-15 Biztonsági javítás kommunikáció	

N: új követelmény

NESAS 2.0 fejlesztés:

1. A beszállítónak rendelkeznie kell olyan eljárásokkal, amelyek biztosítják a harmadik féltől származó komponensek minőségét a termékfejlesztés életciklusa során. A beszállítónak támogatott komponenseket kell választania, és kerülnie kell az élettartamuk végét elérő komponensek használatát.
2. A NESAS2.0 elsősorban a szabványos minőségjavításra optimalizált és CSA-konform.

Közös követelmények

Req.-02 Verziókezelő rendszer, Req.-03 Változáskövetés, Req.-06 Személyzeti oktatás, Req.-09 Információbiztonsági irányítás (ISMS), Req.-19 Folyamatos fejlesztés

SCAS előírások

A SCAS 2.0-ban optimalizálták az általános és a bázisállomási teszteseteket, és kiegészítették a kettős összeköttetésű LTE és 5G titkosítási kulcsok frissítésével a kapcsolat átadása során. Az 5G törzshálózat öt eszközzel egészül ki.

Általános	NodeB	Core								Egyéb
TS 33.117 Általános katalógus követelmények N	TS 33.511 gNodeB	TS 33.512 AMF	TS 33.513 UPF	TS 33.514 UDM	TS 33.515 SMF	TS 33.516 AUSF	N TS 33.520 N3IWF	N TS 33.521 NWDAF	N TS 33.522 SCP	...
	N TS 33.216 eNodeB	TS 33.517 SEPP	TS 33.518 NRF	TS 33.519 NEF	TS 33.116 MME	TS 33.250 PGW	N TS 33.513 IPUPS	N TS 33.326 NSSAAF	...	

HUAWEI

A NESAS követi az EU 5G eszköztárának technikai intézkedéseit

Ilyen például az **eszközbiztonsággal kapcsolatos** követelmények, amelyeket a NESAS maximálisan támogat.

NESAS

Támogatás

5G eszközök biztonsága és tanúsítása

TM 2 — **A biztonsági intézkedések** végrehajtásának biztosítása és értékelése **a meglévő 5G-szabványokban**

TM 4 — **A virtualizált** hálózati funkciók **biztonságának** növelése

TM 7 — A szoftverek **integritásának** megerősítése, **frissítés- és javításkezelés**

TM 8 — A beszállítói folyamatok **biztonsági szabványainak** emelése a szigorú beszerzési feltételek révén

TM 9 — **Az 5G hálózati komponensek**, ügyfélberendezések és/vagy beszállítói folyamatok **EU-tanúsításának** alkalmazása

TM 1 — Az alapvető biztonsági követelmények alkalmazásának biztosítása (biztonságos hálózati **tervezés és architektúra**).

TM 3 — **Szigorú hozzáférés-ellenőrzés** biztosítása

Például:

TM09	**Using EU certification for 5G network components, customer equipment and/or suppliers' processes**	The Commission should consider including into the Union Rolling Work Programme[39] relevant EU-wide scheme(s) for critical network components used in the 5G networks and/or for 5G customer equipment (for example, for eSIMs and related cryptographic material) under the EU certification framework. It should also be examined at a later stage whether the certification or supplier's process could also be added to the Union Rolling Work Programme.	R3 R6 R7	▪ Relevant authorities ▪ EC ▪ ENISA ▪ Stakeholders

Nem kapcsolódik

- O&M biztonság
- Nem-5G
- A telepítés biztonsága
- Reziliencia és folyamatosság

TM5 — Biztonságos 5G **hálózat-menedzsment, üzemeltetés és felügyelet** biztosítása

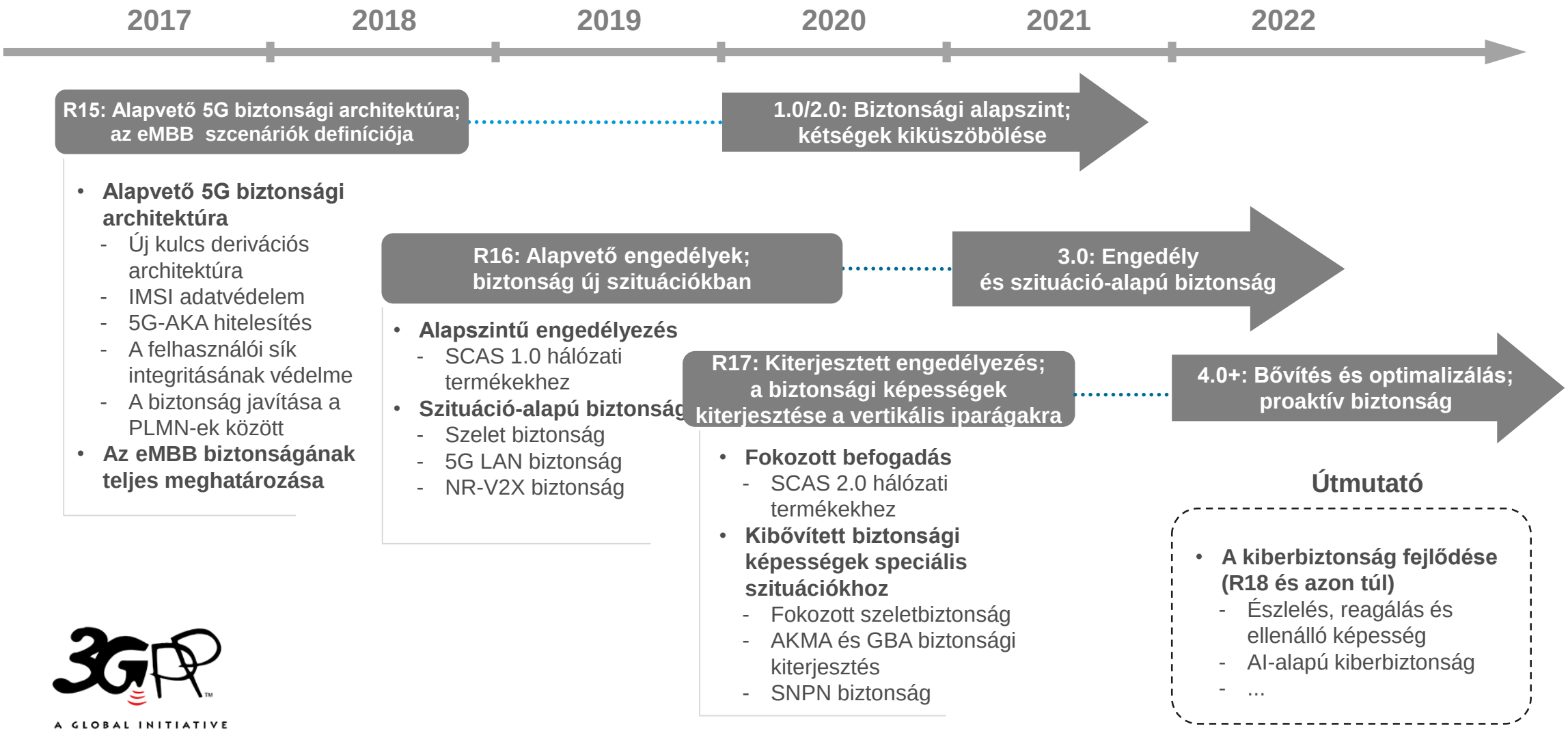
TM6 — **A fizikai biztonság** megerősítése

TM10 — EU-tanúsítás alkalmazása más, **nem 5G-specifikus IKT-termékek,** szolgáltatások (csatlakoztatott eszközök, felhőszolgáltatások) esetében

TM11 — **Az ellenálló-képességi és üzletfolytonossági** tervek megerősítése

HUAWEI

3GPP biztonsági szabványok: Az R15 meghatározza az alapvető 5G biztonsági architektúrát, az R16/R17 pedig folyamatosan bővíti és optimalizálja



3GPP A GLOBAL INITIATIVE

HUAWEI

A NESAS előnyei a mobilkommunikációs ipar szereplői részére

Mobilhálózat-üzemeltetők

- Információk az eszközgyártók és hálózati termékeik **biztonságosságáról** még a beszerzés előtt.
- **Alapszintű biztonsági követelmények** definiálása.
- **Kisebb ráfordítás szükséges a biztonsági teszteléshez,** mivel azt akkreditált tesztlaboratóriumok végzik.

Nemzeti hatóságok és szabályozó szervezetek

- Egy használatra kész **kiberbiztonsági értékelési rendszer.**
- **A hatékony biztonság növelése**, negatív hatások nélkül.
- **Segít elkerülni a** biztonsági követelmények **széttagoltságát a** globális piacon.

Eszközgyártók

- **A biztonsági követelmények betartásának** demonstrálása.
- **A fejlesztési, karbantartási és termékbiztonsági** képességek bemutatása.
- A néha ellentmondásos biztonsági követelmények és a megfelelőség széttagoltságának elkerülése.
- **Hozzáférés a biztonsági követelmények egységes készletéhez**, ami megkönnyíti a hálózati termékfejlesztést és a globális értékesítést.

HUAWEI

A közös felelősségvállalás egyszerre trend és szükségszerűség. A kiberbiztonsági kihívást a közös szabványokon alapuló, összehangolt és ellenőrizhető biztonsági intézkedéseken alapuló együttműködéssel tudjuk kezelni.

Kormány

Jogszabályok és rendeletek kidolgozása,
az E2E felügyelet végrehajtása.

Vállalatok és lakosság

Betartja a jogszabályokat és előírásokat, és követi a jó gyakorlatokat.

Szabványügyi Szervezetek

Meghatározza a követelményeket, szabványokat és a jó gyakorlatokat

IKT-szállítók

Innováció, biztonságos termékek és megoldások fejlesztése

Szolgáltatók és üzemeltetők

Biztonságos és ellenálló hálózat/
ICT/ Megoldás

A távközlésben már régóta **együttműködünk**, felismerve, hogy a **közös felelősségvállalás** ezen modelljei adják a legjobb esélyt arra, hogy olyan biztonságos rendszereket építsünk ki, amelyek világszerte elérhetővé teszik a digitális lehetőségeket az egyének számára.

HUAWEI

Összegzés

1. Az 5G kiberbiztonságának biztosítása a **legfontosabb szereplők**, azaz a hálózatüzemeltetők, a gyártók, az alkalmazásszolgáltatók és a szabályozó hatóságok stb. **közös felelőssége.**

2. A kiberbiztonság felső szintű tervezésének három alapelve: a **mélyreható védelem, a zero-trust@5G** és az **adaptív biztonság**.

3. Az **5G hálózatok számára a NESAS/SCAS megfelelő szabványokat biztosít**: testreszabott, hiteles, globális, hatékony, egységes, nyílt és folyamatosan fejlődő szabványokat. A Huawei támogatja az iparág szabványait, és elsőként teljesítette a NESAS/SCAS vizsgálatokat.

HUAWEI